UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,384	05/24/2001	Shingo Yamaguchi	203223US-28	1503

22850 7590 01/23/2007

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
HA, LEYNNA A	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/863,384	YAMAGUCHI, SHINGO	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 October 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *41-43,45,50-63,65 and 70-80* is/are pending in the application.

4a) Of the above claim(s) *44, 46-49,64, and 66-69* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *41-43,45,50-63,65 and 70-80* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 41-43, 45, 50-63, 65, and 70-80 are pending.

2. In view of the Appeal filed on October 30, 2006, PROSECUTION IS HEREBY REOPENED. A non-Final rejection set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

Gilberto Barron Jr.
SPE 2132

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 41-43, 45, 50-63, 65, and 70-80 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart, et al. (US 6,732,176) and in further view of Lewis (US 6,453,159).

As per claim 41:

Stewart, et al. discusses a method of controlling a network, comprising the steps of:

establishing a computer network connection between a computer and an intermediate device which has network resources connected thereto; **(col.5, lines 2-14 and col.9, lines 30-35; Stewart discloses the access point as the claimed intermediate device.)**

determining a level of security of the computer network connection based on determining whether the computer network connection to connect the computing device to the intermediate device **(col.7, lines 46-61 and col.17, lines 10-15)**, wherein the first level of security is set and a second level of security is set; and **(col.10, lines 20-24)**

controlling a level of access of the computing device to the network resources using the level of security of the computer network connection that has

been determined **(col.7, lines 35-59)**, such that the computing device is allowed access to a first set of network resources **(col.13, lines 2-5 and col.15, lines 64-67)**, including a file server, based on a determined first level of security **(col.16, lines 18-20 and 30-31)**, and is not allowed access to the first set of network resources but is allowed access to a second set of network resources, including access to the Internet and email server, based on a determined second level of security **(col.16, lines 21-29 and col.17, lines 28-32).**

Stewart discloses setting and determining access levels according to the management information base (MIB) such that includes identification information and access information comprises access level or privilege level information (col.7, lines 24-45). The access level information is retrieved and used to determine a user's access to local network resources or Internet access (col.7, lines 55-61). Stewart teaches selectively allowing user access to different parts of the network (col.10, lines 20-24). Stewart teaches the second access level only allows external access such as the Internet (col.13, lines 18-31) where the visitor or customer that includes the access level to gain access to the Internet without being able to view any of the computing resources and file servers (col.16, lines 21-31. This reads on the claimed not allowed access to the first set of network resources but is allowed access to a second set of network resources, including access to the Internet and email server, based on a determined second level of security. Stewart reads on the first level of security where the access level or privilege level that have first access level information indicates which network resources on the local network (col.13, lines 2-6). As mentioned earlier,

Stewart teaches that the second access level corresponds to access to the Internet and not the computing resources and file servers. Thus, it is obvious the second access level is allowed access to the computing resources and the file server is the claimed. Hence, Stewart reads on the claimed controlling a level of access of the computing device to the network resources using the level of security of the computer network connection that has been determined, such that the computing device is allowed access to a first set of network resources, including a file server, based on a determined first level of security.

However, Stewart did not further discuss the computer network connection to connect the computing device to the intermediate device is encrypted, wherein the first level of security is set when it is determined that the computer network connection is encrypted and a second level of security is set when it is determined that the computer network connection is not encrypted.

Lewis teaches the wireless communication system that includes one or more mobile terminals (BMT) and access points connected the system backbone (col.4, lines 15-40). Lewis offers a unique solution to problems of providing encrypting all communications such that BMTs can access the network without engaging in secure encrypted communications (col.5, lines 18-31). Lewis discloses providing levels of encryption where the distribution key server enables authorized BMTs to gain access to the network in secure and non-secure format (col.5, lines 37-67). Stewart obviously discusses the secure access level as encrypted format that provides an ENCRYPT key to the access points and non-secure access level as non-encrypted format (col.9, lines 32-35 and col.13, lines

17-25). Stewart also includes a table which is a list of devices that are authorized to communicate with the network in either an encrypted or a non-encrypted format (col.9, lines 61-64). Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Stewart to include the computer network connection to connect the computing device to the intermediate device is encrypted, wherein the first level of security is set when it is determined that the computer network connection is encrypted as taught by Lewis because an encrypted connection is deemed authorized to communicate securely which prevents access to sensitive information and eavesdropping (col.5, lines 4-17). Further, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Stewart to include a second level of security is set when it is determined that the computer network connection is not encrypted as taught by Lewis because non-encrypted connection is not secure and such non-encrypted manner is for communication link between the mobile terminal and the access point may initially be established (col.10, lines 60-63 and col.13, lines 17-25).

As per claim 42:See Stewart on COL.5, lines 15-19; discusses establishing a wireless computer network connection.

As per claim 43: See Stewart on COL.5, lines 20-21; discusses establishing a wireless computer network connection which conforms to an IEEE 802.11b standard

As per claim 44: Cancelled.

As per claim 45: See Lewis on COL.2, lines 14-24; discusses determining whether the computer network connection is encrypted using Wired Equivalent Privacy ("WEP") encryption

As per claims 46-49: Cancelled

As per claim 50: See Stewart on col.5, lines 5-8 and col.13, lines 44-55; discusses the step of determining is performed by the intermediate device, and said controlling is performed by the intermediate device.

As per claim 51: See Stewart on col.13, lines 44-55; discusses the step of determining is performed by the intermediate device which is a router.

As per claim 52: See Stewart on col.13, lines 44-55 and Lewis on col.15, lines 52-53; discusses the step of controlling is performed by the intermediate device which is a router having a firewall operation.

As per claim 53: See Stewart on col.5, lines 5-8 and col.13, lines 44-55; discusses the step of establishing is performed using the intermediate device which is a router which establishes a wireless connection to the computer.

As per claim 54: See Stewart on col.10, lines 2-3; discusses the step of determining is performed by a server running a network operating system, the server being different from the intermediate device, and the step of controlling is performed by the server running the network operating system.

As per claim 55: See Stewart on COL.7, lines 30-42; discusses the step of determining is performed by the server which is running a network directory service.

As per claim 56: See Stewart on col.13, lines 44-55; discusses the step of

establishing is performed by a bridge connected to the computer through the computer network connection.

As per claim 57: See Stewart on col.13, lines 44-55; discusses the step of establishing is performed by the bridge connected to the computer through the computer network connection which is a wireless network connection.

As per claim 58: See Stewart on col.9, lines 30-46 and Lewis on col.15, lines 52-53; discusses the level of access by a stand-alone firewall device which is connected between the intermediate device and the network resources.

As per claim 59: See Stewart on col.5, lines 44-54; discusses determining the level of security using the intermediate device.

As per claim 60: See Stewart on col.5, lines 5-8; establishing the computer network connection as a wireless connection using the intermediate device.

As per claim 61:

Stewart discloses a system for control a network that includes setting and determining access levels according to the management information base (MIB) such that includes identification information and access information comprises access level or privilege level information (col.7, lines 24-45). The access level information is retrieved and used to determine a user's access to local network resources or Internet access (col.7, lines 55-61). Stewart teaches selectively allowing user access to different parts of the network (col.10, lines 20-24). Stewart teaches the second access level only allows external access such as the Internet (col.13, lines 18-31) where the visitor or customer that includes the

access level to gain access to the Internet without being able to view any of the computing resources and file servers (col.16, lines 21-31. This reads on the claimed not allowed access to the first set of network resources but is allowed access to a second set of network resources, including access to the Internet and email server, based on a determined second level of security. Stewart reads on the first level of security where the access level or privilege level that have first access level information indicates which network resources on the local network (col.13, lines 2-6). As mentioned earlier, Stewart teaches that the second access level corresponds to access to the Internet and not the computing resources and file servers. Thus, it is obvious the second access level is allowed access to the computing resources and the file server is the claimed. Hence, Stewart reads on the claimed controlling a level of access of the computing device to the network resources using the level of security of the computer network connection that has been determined, such that the computing device is allowed access to a first set of network resources, including a file server, based on a determined first level of security.

However, Stewart did not further discuss the computer network connection to connect the computing device to the intermediate device is encrypted, wherein the first level of security is set when it is determined that the computer network connection is encrypted and a second level of security is set when it is determined that the computer network connection is not encrypted.

Lewis teaches the wireless communication system that includes one or more mobile terminals (BMT) and access points connected the system backbone

(col.4, lines 15-40). Lewis offers a unique solution to problems of providing encrypting all communications such that BMTs can access the network without engaging in secure encrypted communications (col.5, lines 18-31). Lewis discloses providing levels of encryption where the distribution key server enables authorized BMTs to gain access to the network in secure and non-secure format (col.5, lines 37-67). Stewart obviously discusses the secure access level as encrypted format that provides an ENCRYPT key to the access points and non-secure access level as non-encrypted format (col.9, lines 32-35 and col.13, lines 17-25). Stewart also includes a table which is a list of devices that are authorized to communicate with the network in either an encrypted or a non-encrypted format (col.9, lines 61-64). Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Stewart to include the computer network connection to connect the computing device to the intermediate device is encrypted, wherein the first level of security is set when it is determined that the computer network connection is encrypted as taught by Lewis because an encrypted connection is deemed authorized to communicate securely which prevents access to sensitive information and eavesdropping (col.5, lines 4-17). Further, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Stewart to include a second level of security is set when it is determined that the computer network connection is not encrypted as taught by Lewis because non-encrypted connection is not secure and such non-encrypted manner is for communication link between the mobile

terminal and the access point may initially be established (col.10, lines 60-63 and col.13, lines 17-25).

As per claim 62: **See Stewart on COL.5, lines 15-19;** discusses establishing a wireless computer network connection.

As per claim 63: **See Stewart on COL.5, lines 20-21;** discusses establishing a wireless computer network connection which conforms to an IEEE 802.11b standard

As per claim 64: **Cancelled.**

As per claim 65: **See Lewis on COL.2, lines 14-24;** discusses determining whether the computer network connection is encrypted using Wired Equivalent Privacy ("WEP") encryption

As per claims 66-69: Cancelled.

As per claim 70: **See Stewart on col.5, lines 5-8 and col.13, lines 44-55;** discusses the means for determining is the intermediate device, and the means for controlling is the intermediate device.

As per claim 71: **See Stewart on col.13, lines 44-55;** discusses the means for determining is the intermediate device which is a router.

As per claim 72: **See Stewart on col.13, lines 44-55 and Lewis on col.15, lines 52-53;** discusses the means for controlling is the intermediate device which is a router having a firewall operation.

As per claim 73: **See Stewart on col.5, lines 5-8 and col.13, lines 44-55;** discusses the means for establishing is the intermediate device which is a router which establishes a wireless connection to the computer.

As per claim 74: **See Stewart on col.10, lines 2-3; 24;** discusses the means for determining is a server running a network operating system, the server being different from the intermediate device, and the means for controlling is the server running the network operating system.

As per claim 75: **See Stewart on COL.7, lines 30-42;** discusses the means for determining is the server which is running a network directory service.

As per claim 76: **See Stewart on col.13, lines 44-55;** discusses the means for establishing is a bridge connected to the computer through the computer network connection.

As per claim 77: **See Stewart on col.13, lines 44-55;** discusses the means for establishing is the bridge connected to the computer through the computer network connection which is a wireless network connection.

As per claim 78: **See Stewart on col.9, lines 30-46 and Lewis on col.15, lines 52-53;** discusses a stand-alone firewall device which is connected between the intermediate device and the network resources.

As per claim 79: **See Stewart on col.5, lines 44-54;** discusses means for determining the level of security using the intermediate device.

As per claim 80: **See Stewart on col.5, lines 5-8;** discusses means for establishing the computer network connection as a wireless connection using the intermediate device.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100